IN THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the Application:

LISTING OF CLAIMS:

1. (Currently Amended) In an intrusion detection system, a[[A]] method of blocking attacks on a computer network, comprising:

receiving, in circuitry of the intrusion detection system, original packets and corresponding retransmit packets from a network, wherein:

each said original packet and corresponding retransmit packet belong to a flow; and

each said original packet and corresponding retransmit packet has a plurality of non-mutable field values;

hashing, in the circuitry of the intrusion detection system, said non-mutable field values of each said original packet to produce a validation signature of each said original packet;

storing, in the circuitry of the intrusion detection system, said validation signatures;

hashing, in the circuitry of the intrusion detection system, said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet;

comparing, in the circuitry of the intrusion detection system, said validation signature to said test signature; and

if said test signature and said validation signature are not identical, terminating said flow by operating a flow terminator circuit of the intrusion detection system.

2. (Original) The method of Claim 1, wherein said storing comprises retaining said validation signatures for a limited time.

3. (Original) The method of Claim 1, wherein said hashing comprises computing a checksum from said non-mutable field values.

4. (Original) The method of Claim 1, wherein said hashing comprises computing a hash value from said non-mutable field values.

5. (Original) The method of Claim 1, wherein said hashing comprises computing a strong hash value from said non-mutable field values.

6. (Original) The method of Claim 1, wherein said hashing comprises computing a cryptographically secure hash value from said non-mutable field values.

7. (Original) The method of Claim 1, wherein said hashing comprises computing a LFSR checksum value using an internal state indicator and said non-mutable field values.

8. (Original) The method of Claim 1, wherein said hashing comprises computing a hash value using a secret number.

9. (Currently Amended) In an intrusion detection system, a[[A]] method of blocking attacks on a computer network, comprising:

generating, in circuitry of the intrusion detection system, a validation signature of an original packet by hashing a plurality of non-mutable field values of said original packet;

generating, in the circuitry of the intrusion detection system, a test signature of a retransmit packet, by hashing a plurality of non-mutable

field values of said retransmit packet, said retransmit packet being a retransmission of said original packet with a flow of packets; and

comparing, in the circuitry of the intrusion detection system, said test signature to said validation signature to determine whether to terminate said flow of packets by operating a flow terminator circuit of the intrusion detection system.

10. (Original) An apparatus for blocking attacks on a computer network, comprising:

means for receiving original packets and corresponding retransmit packets from a network, wherein:

each said original packet and corresponding retransmit packet belong to a flow; and

each said original packet and corresponding retransmit packet has a plurality of non-mutable field values;

first means for hashing said non-mutable field values of each said original packet to produce a validation signature of each said original packet;

means for storing said validation signatures;

second means for hashing said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet, wherein said first means for hashing and said second means for hashing employ the same hashing algorithm;

means for comparing said validation signature to said test signature; and

means for terminating said flow if said test signature and said validation signature are not identical.

11. (Original) The apparatus of Claim 10, wherein said means for storing comprises means for retaining said validation signatures for a limited time.

12. (Original) The apparatus of Claim 10, wherein said first means for hashing and said second means for hashing each comprise means for computing a checksum from said non-mutable field values.

13. (Original) The apparatus of Claim 10, wherein said first means for hashing and said second means for hashing each comprise means for computing a hash value from said non-mutable field values.

14. (Original) The apparatus of Claim 10, wherein said first means for hashing and said second means for hashing each comprise means for computing a strong hash value from said non-mutable field values.

15. (Original) The apparatus of Claim 10, wherein said first means for hashing and said second means for hashing each comprise means for computing a cryptographically secure hash value from said non-mutable field values.

16. (Original) The apparatus of Claim 10, wherein said first means for hashing and said second means for hashing each comprise means for computing a LFSR checksum value using an internal state indicator and said non-mutable field values.

17. (Original) The apparatus of Claim 10, wherein said first means for hashing and said second means for hashing each comprise means for computing a hash value using a secret number.

18. (Original) An apparatus for blocking attacks on a computer network, comprising:

a packet hashing device configured to receive original packets and corresponding retransmit packets from a network, wherein:

each said original packet and corresponding retransmit packet belong to a flow;

each said original packet and corresponding retransmit packet has a plurality of non-mutable field values; and

said packet hashing device employing a packet hashing algorithm to hash said non-mutable field values of each said original packet to produce a validation signature of each said original packet and to hash said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet;

a flow cache connected to said packet hashing device and configured to store said validation signatures;

a comparator operably connected to said flow cache configured to compare said validation signature to said test signature and having an output; and

a flow terminator receiving said output of said comparator and configured to terminate said flow if said output indicates that said test signature and said validation signature are not identical.

19. (Original) The apparatus of Claim 18, wherein said flow cache comprises means for retaining said validation signatures for a limited time.

20. (Original) The apparatus of Claim 18, wherein said packet hashing device comprises means for computing a checksum from said non-mutable field values.

21. (Original) The apparatus of Claim 18, wherein said packet hashing device comprises means for computing a hash value from said non-mutable field values.

22. (Original) The apparatus of Claim 18, wherein said packet hashing device comprises means for computing a strong hash value from said non-mutable field values.

23. (Original) The apparatus of Claim 18, wherein said packet hashing device comprises means for computing a cryptographically secure hash value from said non-mutable field values.

24. (Original) The apparatus of Claim 18, wherein said packet hashing device comprises means for computing a LFSR checksum value using an internal state indicator and said non-mutable field values.

25. (Original) The apparatus of Claim 18, wherein said packet hashing device comprises means for computing a hash value using a secret number.

Claims 26-33 (Canceled).

34. (Original) A computer-readable medium storing a computer program executable by a plurality of server computers, the computer program comprising computer instructions for:

receiving original packets and corresponding retransmit packets from a network, wherein:

each said original packet and corresponding retransmit packet belong to a flow; and

each said original packet and corresponding retransmit packet has a plurality of non-mutable field values;

hashing said non-mutable field values of each said original packet to produce a validation signature of each said original packet;

storing said validation signatures;

hashing said non-mutable field values of each said corresponding retransmit packet to produce a test signature of each said corresponding retransmit packet;

comparing said validation signature to said test signature; and

if said test signature and said validation signature are not identical, terminating said flow.

35. (Original) The computer-readable medium of Claim 34, wherein said computer instructions for storing further comprise computer instructions for retaining said validation signatures for a limited time.

36. (Original) The computer-readable medium of Claim 34, wherein said computer instructions for hashing further comprise computer instructions for computing a checksum from said non-mutable field values.

37. (Original) The computer-readable medium of Claim 34, wherein said computer instructions for hashing further comprise computer instructions for computing a hash value from said non-mutable field values.

38. (Original) The computer-readable medium of Claim 34, wherein said computer instructions for hashing further comprise computer instructions for computing a strong hash value from said non-mutable field values.

39. (Original) The computer-readable medium of Claim 34, wherein said computer instructions for hashing further comprise computer instructions for computing a cryptographically secure hash value from said non-mutable field values.

40. (Original) The computer-readable medium of Claim 34, wherein said computer instructions for hashing further comprise computer instructions for computing a LFSR checksum value using an internal state indicator and said non-mutable field values.

41. (Original) The computer-readable medium of Claim 34, wherein said computer instructions for hashing further comprise computer instructions for computing a hash value using a secret number.

Claims 42-49 (Canceled).

50. (Previously Presented) The method of claim 1 wherein:

receiving original packets and corresponding retransmit packets from a network includes receiving original packets and corresponding retransmit packets from a first network host on an unprotected network across a first network connection; and

the method further comprises:

if said test signature and said validation signature are identical, forwarding said corresponding retransmit packet to a second network host on a protected network across a second network connection, the first and second network hosts being distinct.

51. (Previously Presented) The apparatus of claim 18 wherein the apparatus further comprises:

a first network interface for receiving said original packets and corresponding retransmit packets from a first network host on an unprotected network; and

a second interface for:

transmitting said original packets to a second network host on a protected network, the first and second network hosts being distinct; and

transmitting said corresponding retransmit packets to the second network host if said output indicates that said test signature and said validation signature are identical.